Threatpost | The first stop for security news

- Categories
  - Category List
    - Cloud Security
    - Critical Infrastructure
    - Cryptography
    - Government
  - Category List
    - Hacks
    - Malware
    - Mobile Security
    - Privacy
  - Category List
    - SAS
    - Vulnerabilities
    - Web Security
  - Authors
    - Michael Mimoso
    - Christopher Brook
  - Additional Categories
    - Slideshows
- Featured
  - Authors
    - Michael Mimoso
    - Christopher Brook

Featured Posts

All

Debugging Tool Left on OnePlus Phones,…

Adobe Patches Flash Player, 56 Bugs…

AutoIt Scripting Used By Overlay Malware…

Microsoft Provides Guidance on Mitigating DDE…

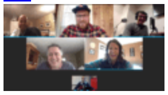
IoT is Insecure, Get Over It!…

Google Patches KRACK Vulnerability in Android

- Podcasts

Latest Podcasts

All


The First Threatpost Alumni Podcast

Threatpost News Wrap Podcast for Nov.…

Threatpost News Wrap Podcast for Nov.…

Threatpost News Wrap, Oct. 20, 2017

Chris Brook Says Farewell to Threatpost

Costin Raiu and Juan Andres Guerrero-Saade…

Recommended

- Videos

Latest Videos

All

Cisco Warns of Critical Flaw in…

Mark Dowd on Exploit Mitigation Development

iOS 10 Passcode Bypass Can Access…

BASHLITE Family Of Malware Infects 1…

How to Leak Data From Air-Gapped…

Bruce Schneier on the Integration of…

Recommended

- Twitter
- Facebook
- Google
- LinkedIn
- YouTube
- RSS

Search □

Join thousands of people who receive the latest breaking **cybersecurity news** every day.

E-mail

Sign Up

Welcome > Blog Home>Cryptography > Crooks Switch from Ransomware to Cryptocurrency Mining

162 0 0 0 2

Crooks Switch from Ransomware to Cryptocurrency Mining

by Tom Spring December 21, 2017 , 5:30 pm

Criminals behind the VenusLocker ransomware have switched to cryptocurrency mining in their latest campaign targeting computer users in South Korea. Instead of attempting to infect targeted computers with ransomware, the group is now trying to install malware on PCs that mines for Monero, an open-source cryptocurrency.

The shift was spotted by FortiGuard Labs, which said the group behind the attacks is attempting to capitalize on a surging cryptocurrency market.

Related Posts

Ad Network Circumvents Ad-Blocking Tools To Run In-Browser Cryptojacker Scripts

March 1, 2018 , 12:40 pm

U.K. and U.S. Government Websites Among Thousands Infected by Cryptocurrency Miner

February 12, 2018 , 12:28 pm

Insurance Customers' Personal Data Exposed Due to Misconfigured NAS Server

February 8, 2018 , 2:51 pm

"With more and more people realizing that cryptocurrency is potentially a significantly profitable investment, this rise is likely to continue for the foreseeable future. And where there is profit, that is where malware attacks will gather," wrote FortiGuard in a report Wednesday.

Researchers said the shift by threat actors is also spurred by anti-ransomware mitigation efforts that have made infecting systems with malware harder.

"This past October Microsoft added a Controlled folder access feature to Windows Defender Security for Windows 10 users to prevent malicious (or unexpected) alteration of important files. Features such as this can effectively thwart ransomware attacks. Which is probably part of the reason why the threat actors behind VenusLocker decided to switch targets," researchers said.

Why Monero crypto currency, and not the surging Bitcoin? According to FortiGuard, Monero's mining algorithm is designed for ordinary computers. Bitcoin, on the other hand, requires higher-end systems equipped with Application-Specific Integrated Circuits or high-end GPUs, according to researchers.

"The second reason is Monero's promise of transaction anonymity. With Bitcoin, a wallet is a public record," researchers wrote. Monero's wallet uses "stealth addresses" along with "transaction mixing" allowing criminals to cloak account activity.

Those behind VenusLocker, and now Monero mining malware, are targeting South Korean users via phishing campaigns. Emails contain malicious attachments compressed in EGG archive format, developed by ESTsoft, a South Korean tech firm.

Ploys range from fake messages from a website insisting recipients open an accompanying attachment that contains important personal breach information pertaining to a recent website hack. Another message insists a recipient open the malicious attachment in order to view copyright protected images illegally used on the target's website.

"Once the malware is executed, an embedded binary of the Monero CPU miner XMRig v2.4.2 is executed. As a basic attempt to hide this resource hogging operation, the miner is executed as a remote thread under the legitimate Windows component wuapp.exe, which is executed beforehand to avoid raising suspicions," researchers describe.

Researchers also noted many similarities between the hidden file attribute and shortcut files used to trick users in the VenusLocker malware and the mining malware.

"An interesting observation is that this same scheme has been used by VenusLocker in the past. To confirm this assumption, we had to take a closer look at the shortcut files' metadata, and sure enough, we found a direct relation to the ransomware. Aside from the target paths, the shortcut files used during the VenusLocker ransomware period are practically identical to the ones being used in this campaign," researchers said.

FortiGuard researchers say the switch to crytocurrency mining by ransomware crooks is a growing trend that could extend into 2018. "With cryptocurrency values being more enticing than ever, it is a real possibility," they said.

162 0 0 0 2

Categories: Cryptography, Hacks, Malware, Privacy

Comments (2)

1. *Marco Garcia* January 5, 2018 @ 7:26 am
   1

   There is a long list of idiots who are more than willing to download software to their laptops and cellphones to "mine" while they are sleeping, completely oblivious to the threats they are exposing themselves to, with the false belief they will be obtaining free money or altcoin(s).

   Reply ↓
2. *Gwen Collier* January 9, 2018 @ 12:33 pm
   2

   What can I download to do away with this vulnerability. I am not seeing that information so we can read and read and be warned but WHAT can we do about it?

   Reply ↓

Leave A Comment

Your email address will not be published. Required fields are marked *

Comment

You may use these HTML tags and attributes: `<a href="" title=""> <abbr title=""> <acronym title=""> <b> <blockquote cite=""> <cite> <code> <del datetime=""> <em> <i> <q cite=""> <s> <strike> <strong>`

Name

Email

Post Comment

I'm not a robot

reCAPTCHA
Privacy - Terms

□ Notify me when new comments are added.

Recommended Reads

88 0 0 0 0

March 1, 2018 , 12:40 pm
Categories: Malware, Privacy, Web Security

Ad Network Circumvents Ad-Blocking Tools To Run In-Browser Cryptojacker Scripts

by Lindsey O'Donnell

Researchers say cyrptojackers are bypassing ad-blocking software in an attempt to run in-browser cyrptocurrency miner Coinhive.

Read more...

110 0 0 0 0

February 12, 2018 , 12:28 pm

Categories: Hacks, Vulnerabilities, Web Security

U.K. and U.S. Government Websites Among Thousands Infected by Cryptocurrency Miner

by Christopher Kanaracus

The attack could have been averted through a technique called subresource integrity, according to researcher Scott Helme.

Read more...

142 0 0 0 0

February 8, 2018 , 2:51 pm
Categories: Cloud Security, Privacy, Vulnerabilities, Web Security

Insurance Customers' Personal Data Exposed Due to Misconfigured NAS Server

by Christopher Kanaracus

The vulnerability also exposed login credentials for a massive national insurance claims database, Upguard says.

Read more...

Top Stories

Olympic Destroyer: A False Flag Confusion Bomb

March 8, 2018 , 12:01 pm

Sofacy APT Adopts New Tactics and Far East Targets

March 9, 2018 , 12:11 pm

Vulnerability in Robots Can Lead To Costly Ransomware Attacks

March 9, 2018 , 9:01 am

Supporters of Net Neutrality Vow to Fight Rule Changes

February 23, 2018 , 8:31 am

Google Patches 11 Critical Bugs in March Android Security Bulletin

March 6, 2018 , 1:34 pm

IoT Security Disconnect: As Attacks Spike, Device Patching Still Lags

March 6, 2018 , 12:43 pm

Equifax Adds 2.4 Million More People to List of Those Impacted By 2017 Breach

March 2, 2018 , 3:12 pm

Ad Network Circumvents Ad-Blocking Tools To Run In-Browser Cryptojacker Scripts

March 1, 2018 , 12:40 pm

Join thousands of people who receive the latest breaking **cybersecurity news** every day.

E-mail

Sign Up

- RSS Feeds
- Home
- About Us
- Contact Us

Categories
Black HatCloud SecurityCritical InfrastructureCryptographyFeaturedGovernmentHacksIoTMalwareMobile SecurityPodcastsPrivacySecurity Analyst SummitSlideshowUncategorizedVideosVulnerabilitiesWeb Security

Authors

Michael Mimoso
Tom Spring
Christopher Brook

Threatpost | The first stop for security news

- Terms of Service
- Privacy